



Software Diversification for WebAssembly

JAVIER CABRERA-ARTEAGA

Doctoral Thesis in Computer Science
Supervised by
Benoit Baudry and Martin Monperrus

Stockholm, Sweden, 2023

KTH Royal Institute of Technology
School of Electrical Engineering and Computer Science
Division of Software and Computer Systems
SE-10044 Stockholm
Sweden

TRITA-EECS-AVL-2020:4
ISBN 100-

Akademisk avhandling som med tillstånd av Kungl Tekniska högskolan framlägges
till offentlig granskning för avläggande av Teknologie doktorexamen i elektroteknik
i .

© Javier Cabrera-Arteaga , date

Tryck: Universitetsservice US AB

Abstract

Keywords: Lorem, Ipsum, Dolor, Sit, Amet

Sammanfattning

LIST OF PAPERS

1. ***WebAssembly Diversification for Malware Evasion***
Javier Cabrera-Arteaga, Tim Toady, Martin Monperrus, Benoit Baudry
Computers & Security, Volume 131, 2023, 17 pages
<https://www.sciencedirect.com/science/article/pii/S0167404823002067>
2. ***Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly***
Javier Cabrera-Arteaga, Nicholas Fitzgerald, Martin Monperrus, Benoit Baudry
Under review, 17 pages
<https://arxiv.org/pdf/2309.07638.pdf>
3. ***Multi-Variant Execution at the Edge***
Javier Cabrera-Arteaga, Pierre Laperdrix, Martin Monperrus, Benoit Baudry
Moving Target Defense (MTD 2022), 12 pages
<https://dl.acm.org/doi/abs/10.1145/3560828.3564007>
4. ***CROW: Code Diversification for WebAssembly***
Javier Cabrera-Arteaga, Orestis Floros, Oscar Vera-Pérez, Benoit Baudry, Martin Monperrus
Measurements, Attacks, and Defenses for the Web (MADWeb 2021), 12 pages
<https://doi.org/10.14722/madweb.2021.23004>
5. ***Superoptimization of WebAssembly Bytecode***
Javier Cabrera-Arteaga, Shrinish Donde, Jian Gu, Orestis Floros, Lucas Satabin, Benoit Baudry, Martin Monperrus
Conference Companion of the 4th International Conference on Art, Science, and Engineering of Programming (Programming 2021), MoreVMs, 4 pages
<https://doi.org/10.1145/3397537.3397567>
6. ***Scalable Comparison of JavaScript V8 Bytecode Traces***
Javier Cabrera-Arteaga, Martin Monperrus, Benoit Baudry
11th ACM SIGPLAN International Workshop on Virtual Machines and Intermediate Languages (SPLASH 2019), 10 pages
<https://doi.org/10.1145/3358504.3361228>

ACKNOWLEDGEMENT

Contents

List of Papers	iii
Acknowledgement	iv
Contents	1
I Thesis	2
1 Introduction	3
1.1 The risks of WebAssembly monoculture	4
1.2 Problems statements	5
1.3 Software Diversification	6
1.4 Summary of research papers	7
2 Background and state of the art	10
2.1 WebAssembly	10
2.1.1 From source code to WebAssembly	11
2.1.2 Extending WebAssembly	14
2.1.3 WebAssembly's binary format	14
2.1.4 WebAssembly's runtime	15
2.1.5 WebAssembly's control-flow	17
2.1.6 Security and Reliability for WebAssembly	18
2.1.7 Open challenges	20
2.2 Software diversification	20
2.2.1 Generation of Software Variants	20
2.2.2 Equivalence Checking	23
2.2.3 Variants deployment	24
2.2.4 Software Diversification Assessment	25
2.2.5 Offensive Diversification	26
2.2.6 Open challenges	27

3	Automatic Software Diversification for WebAssembly	29
3.1	CROW: Code Randomization of WebAssembly	30
3.1.1	Enumerative synthesis	31
3.1.2	Constant inferring	32
3.1.3	Exemplifying CROW	33
3.2	MEWE: Multi-variant Execution for WebAssembly	35
3.2.1	Multivariant call graph	36
3.2.2	Exemplifying a Multivariant binary	36
3.3	WASM-MUTATE: Fast and Effective Binary Diversification for WebAssembly	39
3.3.1	WebAssembly Rewriting Rules	40
3.3.2	E-Graphs traversals	41
3.3.3	Exemplifying WASM-MUTATE	42
3.4	Comparing CROW, MEWE, and WASM-MUTATE	44
3.4.1	Security applications	47
4	Exploiting Software Diversification for WebAssembly	49
4.1	Offensive Diversification: Malware evasion	49
4.1.1	Cryptojacking defense evasion	50
4.1.2	Methodology	51
4.1.3	Results	53
4.2	Defensive Diversification: Speculative Side-channel protection	56
4.2.1	Threat model: speculative side-channel attacks	58
4.2.2	Methodology	58
4.2.3	Results	60
5	Conclusions and Future Work	65
5.1	Summary of technical contributions	65
5.2	Summary of empirical findings.	66
5.3	Future Work	67
II	Included papers	70
	Superoptimization of WebAssembly Bytecode	72
	CROW: Code Diversification for WebAssembly	73
	Multi-Variant Execution at the Edge	74
	WebAssembly Diversification for Malware Evasion	75

CONTENTS

3

Wasm-mutate: Fast and Effective Binary Diversification for WebAssembly **76**

Scalable Comparison of JavaScript V8 Bytecode Traces **77**

Part I

Thesis